ProToken Plus & SafeSign Client Standard

Guia de Instalação e Utilização

Pronova Consultoria em Tecnologia da Informação Ltda.

Todos os produtos da Pronova Soluções Inteligentes (PRONOVA) incluindo, sem limitar-se a, cópias de avaliação, disquetes, CD-ROMs, hardware, software e documentação, e todos os futuros pedidos, estão sujeitos aos termos desta Licença. Se você não está de acordo com os termos aqui expostos, por favor, proceda a devolução do pacote completo e dentro do prazo de quinze dias úteis e reembolsaremos o custo do produto, exceto o frete e os encargos administrativos. Ao utilizar o produto você declara conhecer e aceitar os termos e condições do presente, que se formalizará em um contrato de Licença entre você e a PRONOVA, que também terá alcance aos distribuidores, revendas ou representantes da PRONOVA, com o alcance aqui convencionado.

1. Uso Permitido – Você pode fundir, relacionar e/ou fazer link do Software com outros programas com o único propósito de proteger esses programas de acordo com o uso descrito no Guia do Desenvolvedor que está junto com o produto, ou que pode ser encontrado no site web da PRONOVA (www.pronova.com.br). Você pode realizar cópias do Software com o fim de utilizá-las como cópias de segurança ou backup.

2. Uso proibido – -O Software ou o hardware fornecido pela PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desasemblada, descompilada, revisada, melhorada e modificada de qualquer forma, exceto como especificamente se permite no presente. Você não pode praticar engenharia reversa ao Software ou qualquer parte do produto, ou tentar descobrir o código fonte do Software. Você não pode usar o meio ótico ou magnético incluído com o produto com o propósito de transferir ou guardar dados que não fazem parte original de Produto, ou uma melhora ou atualização de Produto fornecida pela PRONOVA.

3. Garantia – PRONOVA garantem que os Produtos e os meios de armazenamento de Software são substancialmente livres de defeitos de fabricação ou materiais. Esta garantia terá validez por um período de tempo de doze (12) meses desde a entrega de produto por parte da PRONOVA.

4. Fim da garantia – No caso de que ocorra qualquer fato que produza o fim da garantia, a única obrigação por parte da PRONOVA é efetuar ou reparar a descrição da PRONOVA, qualquer produto sem que isto possa gerar algum encargo para você.

Para tanto PRONOVA ou revendas autorizadas, não serão responsáveis em nenhum caso por nenhum dano, prejuízo, gasto, ou conceito sobre a garantia expressamente reconhecida no presente. Em conseqüência a responsabilidade total faz de você ou qualquer terceiro por qualquer causa, tanto contratual como extracontratual, incluindo dolo, culpa ou negligência, não excederá, em nenhum caso, do preço que você pagou pelo Produto que tenha causado um dano, ou que tenha sido objeto de, ou indiretamente relacionado com, a causa do dano.

Em nenhum caso PRONOVA é responsável por nenhum dano causado por culpa ou negligência sua ou de terceiros, nem por nenhuma perda de dados, ganhos ou economias, ou por outros danos casuais ou casualidades, mesmo se PRONOVA tiver avisado da possibilidade de ocorrência ao dano. Qualquer produto que você entregará a PRONOVA com a finalidade de troca em comprimento desta garantia, passará a ser propriedade da PRONOVA

5. Limitação da Garantia – A presente garantia não cobre e nem cobrirá defeitos provocados por uso inadequado ou conservação do produto. A garantia também se perderá se for verificado que o produto foi, de qualquer modo, aberto, forçado, desarmado ou que tenha sido feito qualquer um dos Usos Proibidos detalhados no presente.

Para invocar a garantia, é necessário se comunicar por escrito com a PRONOVA, durante o período de garantia, previsto da presente garantia e a nota fiscal de compra do produto. PRONOVA terão direito de avaliar o produto em até 15 dias, ou por um prazo maior desde que o defeito seja importante. Qualquer produto que você devolver a PRONOVA deverá ser enviado com frete e seguro pré-pago.

Exceto as condições expostas, PRONOVA não ortoga outra garantia dos produtos do que as expressamente detalhadas no presente. Para tanto não poderá se estender que exista extensão ou maior alcance da mesma, tanto expressa com implícita, incluindo, podem sem limitar-se a possibilidade do uso do produto para um propósito em particular.

6. Término da Garantia – Esta licença será considerada automaticamente terminada em qualquer caso em que você não cumprir total ou parcialmente os termos deste contrato.

Índice

Política de Garantia Pronova

IMPORTANTE-LEIA ESTA GARANTIA DO FABRICANTE COM ATENÇÃO PARA ENTENDER SEUS DIREITOS E OBRIGAÇÕES! O termo "Dispositivo de Hardware" significa o produto de hardware Pronova. O termo "Você" significa uma pessoa física ou jurídica que será referida nesta Garantia Limitada como *"Você"* e "Seu(s)/Sua(s)".

A. GARANTIAS.

1. Garantia Expressa. *Você* estará sujeito aos termos e condições desta Garantia Limitada e, em substituição a quaisquer outras (se houver) garantias expressas, a Pronova garante a *Você,* sob condições normais de uso e serviço, na data da aquisição identificada no recibo ou no comprovante de pagamento e pelo período de tempo especificado abaixo para o Dispositivo de Hardware aplicável (doravante denominados o "Prazo de Garantia"), que o Dispositivo de Hardware será executado substancialmente em conformidade com o descrito na embalagem e na documentação da Pronova que o acompanha. Relativamente ao descobrimento de defeitos após o Prazo de Garantia, a Pronova não fornecerá qualquer tipo de garantia ou condição.

A PRONOVA assegura total cobertura contra defeito de fabricação para os produtos fornecidos ao cliente no território brasileiro, durante o período da garantia.

Prazo de Garantia

Garantia Legal - 90 (noventa) dias

A garantia legal praticada pela PRONOVA obedece aos dispositivos relacionados no artigo 26 do Código de Defesa do Consumidor (CDC), e é direito do consumidor que apresente a reclamação comprovadamente formulada no prazo de 90 (noventa) dias da data de aquisição do produto PRONOVA para troca do produto e/ou serviço adquirido por igual ou equivalente superior.

A reposição dos produtos em garantia estará sujeita às condições de retorno do produto, observando a garantia legal, conforme art. 50 do CDC.

PRAZO TOTAL DA GARANTIA:

(I) Para todos os conjuntos de Tokens USB: 90 (noventa) dias;

(II) Leitor de cartão inteligente: 90 (noventa) dias;

(III) Cartão Inteligente: 90 (noventa) dias.

CONCORDANDO COM A GARANTIA CONTRATUAL, O CONSUMIDOR ABRE MÃO DE QUAISQUER RECLAMAÇÕES APÓS O PERÍODO DE 90 (noventa) DIAS, TEMPO CONSIDERADO SUFICIENTE PARA A IDENTIFICAÇÃO DE QUAISQUER PROBLEMAS NO PRODUTO OU NA PRESTAÇÃO DE SERVIÇOS.

Os dispositivos criptográficos (tokens e cartões) e leitores de cartão inteligente vendidos pela PRONOVA têm garantia contra defeitos de fabricação pelo prazo de 90 (noventa) dias contados a partir da data de aquisição do produto PRONOVA.

Os dispositivos criptográficos (tokens e cartões) armazenam o seu Certificado Digital protegendo-o contra acessos indevidos. AS SENHAS (PIN, PUK, SENHA, FRASE SENHA OU PASSWORD) PARA ACESSO A ESSES DISPOSITIVOS SÃO SOMENTE DE CONHECIMENTO E RESPONSABILIDADE DO TITULAR OU RESPONSÁVEL DO CERTIFICADO DIGITAL, E A PRONOVA NÃO MANTÉM CÓPIAS OU POSSUI MEIOS DE RECUPERÁ-LAS.

CASO O DISPOSITIVO CRIPTOGRÁFICO SEJA BLOQUEADO OU INUTILIZADO DEVIDO À PERDA DAS SENHAS, SEU CONTEÚDO SERÁ PERDIDO. A REPOSIÇÃO DESTES DISPOSITIVOS (E DE SEU CONTEÚDO) NÃO É COBERTA PELA POLÍTICA DE GARANTIA PRONOVA.

Caso o Serviço de Suporte Técnico PRONOVA constate defeito de fabricação que requeira a substituição do dispositivo criptográfico durante o período de vigência desta garantia, a PRONOVA:

- Efetuará troca do dispositivo criptográfico, sem custo adicional para o cliente; e

- Não emitirá um novo certificado, sem custo adicional para o cliente, caso o defeito de fabricação acarrete na perda do Certificado Digital.

Essa Garantia Limitada não cobrirá, bem como não será fornecido qualquer tipo de garantia para aspectos subjetivos ou estéticos do Dispositivo de Hardware. A garantia expressa prevista acima constitui a única garantia expressa concedida a Você e é fornecida em substituição a

todas as outras condições e garantias, sejam expressas ou implícitas (exceto quaisquer garantias implícitas existentes que não possam ser recusadas), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Qualquer informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, não criará qualquer garantia ou condição ou ampliará o escopo desta Garantia Limitada.

2. Limitação da Vigência das Garantias Implícitas. Se Você for um consumidor estrangeiro, também poderá ter uma condição e/ou garantia implícita de acordo com a legislação de algumas jurisdições, a qual é limitada pela vigência do presente Prazo de Garantia.

B. RECURSO EXCLUSIVO. Sujeito à legislação aplicável e às disposições a seguir, e desde que Você, durante o Prazo de Garantia, devolva o Dispositivo de Hardware à Pronova, com uma cópia do recibo ou comprovante válido de pagamento, a Pronova irá, a seu critério:

(i) reparar ou substituir o Dispositivo de Hardware; ou (ii) indenizá-lo pelos danos diretos sofridos por Você, limitando-se a responsabilidade ao valor efetivamente pago por Você pelo Dispositivo de Hardware.

(ii) Qualquer Dispositivo de Hardware reparado ou substituído conforme esta Garantia Limitada terá garantia pelo Prazo de Garantia original remanescente ou por 30 (trinta) dias, a partir da data de devolução do item para Você, o que for maior.

Salvo previsão expressa em contrário pela legislação aplicável, Você deverá arcar com os custos relacionados ao transporte (inclusive embalagem) do produto dentro do prazo da garantia; e

C. ISENÇÃO DE OUTRAS GARANTIAS. A garantia expressa especificada acima é a única garantia expressa oferecida a Você e é fornecida em substituição a todas as outras condições e garantias expressas ou implícitas (se houver), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Nenhuma outra garantia é fornecida em relação ao Dispositivo de Hardware ou aos serviços de garantia por qualquer pessoa, incluindo, mas não se limitando a, a Pronova, os seus agentes, as afiliadas e os fornecedores. Nenhuma informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, deverá criar uma garantia ou condição ou ampliar o escopo desta Garantia Limitada. Também não há garantias ou condições de

titularidade, uso pacífico ou não-violação de direitos de autor no Dispositivo de Hardware.

D. EXCLUSÃO DE OUTROS DANOS.

NA EXTENSÃO MÃXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, A PRONOVA, SEUS AGENTES, AFILIADAS E/OU FORNECEDORES NÃO SERÃO RESPONSÁVEIS POR QUALQUER:

(i) DANO CONSEQÜENCIAL OU INCIDENTAL;

(ii) DANOS POR LUCROS CESSANTES, INTERRUPÇÃO DE NEGÓCIOS, PERDA DE DADOS, INFORMAÇÕES CONFIDENCIAIS OU OUTRAS, PERDA DE PRIVACIDADE, QUALQUER INABILIDADE NO USO DO DISPOSITIVO DE HARDWARE, NO TODO OU EM PARTE, DANOS PESSOAIS OU QUALQUER FALHA NO CUMPRIMENTO DE QUALQUER OBRIGAÇÃO (INCLUINDO MAS NÃO SE LIMITANDO A QUALQUER OBRIGAÇÃO GERADA EM RELAÇÃO A CASO DE NEGLIGÊNCIA E QUEBRA DO PRINCÍPIOS DE BOA-FÉ E DO ESFORÇO DE APRIMORAMENTO);

(iii) DANO INDIRETO, ESPECIAL OU PUNITIVO DECORRENTE DO OU DE QUALQUER FORMA RELACIONADO COM O DISPOSITIVO DE HARDWARE.

(iii) QUALQUER TIPO DE INFORMAÇÃO QUE VENHA A SER ARMAZENADA NOS EQUIPAMENTOS COMERCIALIZADOS PELA PRONOVA.

AS EXCLUSÕES ACIMA SERÃO APLICADAS MESMO QUE A PRONOVA OU QUALQUER AGENTE, AFILIADA OU FORNECEDOR TENHA SIDO ALERTADO SOBRE A POSSIBILIDADE DE OCORRÊNCIA DE TAIS PERDAS OU DANOS, E MESMO QUE HAJA FALHA, DANO (INCLUSIVE NEGLIGÊNCIA), RESPONSABILIDADE OBJETIVA OU PELO FATO DO PRODUTO, DECLARAÇÃO FALSA OU QUALQUER OUTRO MOTIVO.

E. EXCLUSÕES DE COBERTURA. A Garantia Limitada não será aplicável e a Pronova, seus agentes, afiliadas e/ou fornecedores não terão qualquer responsabilidade relativa a esta Garantia Limitada se o Dispositivo de Hardware:

(i) for usado para fins comerciais (inclusive aluguel ou arrendamento);

(ii) for modificado ou adulterado;

(iii) for danificado por motivos de força maior, alta-tensão, uso indevido, abuso, negligência, acidente, desgaste, manipulação indevida, aplicação errada ou outras causas não

relacionadas a defeitos no Dispositivo de Hardware;

(iv) for danificado por programas, informações, vírus ou arquivos ou durante envios ou transmissões;

(v) não for usado de acordo com a documentação e as instruções de uso que o acompanham; ou

(vi) for reparado, modificado ou alterado por outra pessoa que não seja um representante da assistência técnica autorizada da Pronova e se a assistência técnica não autorizada causar ou contribuir para o surgimento de qualquer defeito ou dano.

F. REGISTRO. Não é necessário registrar a aquisição do Dispositivo de Hardware para que essa Garantia Limitada tenha validade.

G. BENEFICIÁRIO. Na extensão máxima permitida pela lei aplicável, a Garantia Limitada será concedida exclusivamente a Você, o primeiro adquirente do Dispositivo de Hardware, não existindo outros beneficiários da Garantia Limitada. Salvo previsão expressa em contrário na lei, esta Garantia limitada não será destinada, bem como não será aplicável a qualquer outra pessoa, inclusive qualquer pessoa para a qual Você faça uma transferência do Dispositivo de Hardware.

H. INFORMAÇÕES ADICIONAIS. A Pronova é a entidade que fornece esta Garantia Limitada. Para receber instruções sobre como executar esta Garantia Limitada, entre em contato com uma subsidiária Pronova de sua localidade ou escreva para; Pronova Soluções Inteligente, Avenida das Américas 500, bloco 4, sala 302, Barra da Tijuca, Rio de Janeiro, RJ, CEP 22.640-100, ou visite a Pronova na Internet no endereço http//www.pronova.com.br

Outras exigências:

1. Você deverá enviar um comprovante de pagamento na forma de uma fatura (ou uma cópia) ou um recibo autêntico com data evidenciando que Você é o beneficiário desta Garantia Limitada e que a Sua solicitação está sendo feita dentro do Prazo de Garantia.

2. Para execução da Garantia Limitada, Você deverá levar ou enviar o item na sua embalagem original ao local especificado pela Pronova. Salvo previsão expressa em contrário prevista na legislação aplicável, Você arcará com os custos relacionados ao transporte (inclusive embalagem) do serviço dentro do prazo da garantia.

Caso não siga as instruções acima, Você poderá ter despesas adicionais, poderá perder a sua garantia ou poderão ocorrer atrasos.

As informações contidas neste documento, incluindo URLs e outras referências a sites na Internet, estão sujeitas a alterações sem aviso prévio. Salvo indicação em contrário, os exemplos de empresas, organizações, produtos, nomes de domínio, endereços de email, logotipos, pessoas, lugares e acontecimentos aqui mencionados são fictícios e nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de e-mail, logotipo, pessoa ou acontecimento real é intencional ou deve ser inferida.

Obedecer a todas as leis de direitos autorais aplicáveis é responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa e por escrito da Pronova.

A Pronova pode ter patentes ou requisições para obtenção de patente, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual que abrangem o conteúdo deste documento. A posse deste documento não lhe confere nenhum direito sobre as citadas patentes, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual, salvo aqueles expressamente mencionados em um contrato de licença, por escrito, da Pronova.

Pronova é marca registrada ou comercial da Pronova Consultoria em Tecnologia da Informação Ltda. na República Federativa do Brasil e/ou em outros países.

Os nomes de produtos e de empresas reais aqui mencionados podem ser marcas comerciais de seus respectivos proprietários.

A Pronova concede ao comprador deste produto o direito de reproduzir uma (1) cópia do "Manual de Instruções" impresso para cada Dispositivo de Hardware adquirido na embalagem.

1. Glossário

Assinatura Digital: Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê os seguintes serviços de segurança: autenticação da origem, integridade de dados e não repudiação do signatário;

Atribuição de chaves (key establishment): Processo que possibilita atribuir uma chave simétrica para uso criptográfico aos participantes legítimos de uma sessão de comunicação. A atribuição de chaves pode ser realizada por meio de duas técnicas: "Negociação de Chaves" ou "Transferência de Chaves";

Autoridade Certificadora (AC): Entidade idônea autorizada a emitir, renovar e cancelar certificados digitais. É responsável pela administração das chaves públicas;

Autoridade de Registro (AR): É uma entidade operacionalmente vinculada à determinada Autoridade Certificadora Habilitada, responsáveis pela confirmação da identidade dos solicitantes dos certificados e-CPF e e-CNPJ;

Certificado Digital: Documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública;

Chave criptográfica: Código ou parâmetro usado em conjunto com um algoritmo criptográfico, determinando as seguintes operações:

- Transformação de dados em texto claro para um formato cifrado e vice-versa;
- Assinatura digital computada a partir de dados;
- Verificação de uma assinatura digital computada a partir de dados;
- Geração de um código de autenticação computado a partir de dados; ou
- Um acordo para troca de um segredo compartilhado;

Chave Criptográfica em texto claro: representa uma chave criptográfica não cifrada;

Chave secreta: Chave criptográfica, usada com um algoritmo criptográfico de chave secreta, que está unicamente associada a uma ou mais entidades e não deveria tornar-se pública;

Código de Autenticação: corresponde a um verificador de integridade criptográfico que é comumente referenciado como MAC (Message Authentication Code);

Co-assinatura: A co-assinatura (ou sign) é aquela gerada independente das outras assinaturas;

Contra-assinatura: A contra-assinatura (ou countersign) é aquela realizada sobre uma assinatura já existente. Na especificação PKCS#7, a contra-assinatura é adicionada na forma de um atributo não autenticado (countersignature attribute) no bloco de informações (signerInfo) relacionado a assinatura já existente;

Elemento de Dado: Corresponde a um item de informação para o qual são definidos um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4];

Entidade usuária externa: Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido;

ePassNG: Nova geração de produto (middleware framawork) desenvolvido pela Feitian. Este novo middleware suporta todas as séries dos produtos ePass. Fácil de ser atualizado com novo suporte de hardware, bem como suporte a aplicações PKI;

FIPS (Federal Information Processing Standards): correspondem a padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS, quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade, e não há padrões ou soluções industriais aceitáveis;

Firmware: Programas e componentes de dados de um módulo que estão armazenados em hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) e não podem ser dinamicamente escritos ou modificados durante a execução;

Fronteira criptográfica (cryptographic boundary): A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.

Hardware: Parte ou equipamento físico usado para processar programas e dados;

ICP-Brasil: conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras;

Identificador de Registro: Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4];

Integridade: propriedade que determina que dados não devem ser modificados ou apagados de uma maneira não autorizada e indetectável;

Interface: representa um ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos módulos criptográficos;

Interface CryptoAPI: Interface de operação de criptografia desenvolvida pela Microsoft. Esta interface oferece ao dispositivo idenpendência ou implementação de encapsulamento de algoritmos criptográficos, permitindo aos desenvolvedores uma fácil utilização destes algoritmos em suas aplicações PKI, incluindo criptografia de dados, verificação de certificados e assinatura digital na plataforma Windows;

ITI: autarquia federal vinculada à Casa Civil da Presidência da República. O ITI é a Autoridade Certificadora Raiz - **AC Raiz** da Infra-Estrutura de Chaves Públicas Brasileira - **ICP-Brasil**. Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

Middleware: Software que é usado amarrar uma aplicação;

Módulo criptográfico (cryptographic module): Conjunto de hardware, software e/ou firmaware que implementa funções ou processos criptográficos, abrangendo algoritmos criptográficos e de geração de chaves;

Módulo criptográfico de chip único (Single-chip Cryptographic Module): representa uma materialização física na qual um chip único de circuito integrado (Integrated Circuit Chip - ICC) poderia ser usado como dispositivo independente (standalone), ou poderia estar embutido/confinado dentro de um produto (material de área delimitada), que está ou não fisicamente protegido. Por exemplo, módulos criptográficos de chip único incluem os cartões inteligentes (Smart Cards);

Negociação de chaves (key agreement): Protocolo que possibilita atribuir uma chave simétrica aos participantes legítimos em função de valores secretos definidos por cada um dos participantes, de forma que nenhum dos participantes possa predeterminar o valor da chave. Neste método, a chave não é transferida, nem mesmo de forma cifrada. Exemplo clássico desta classe de protocolo é o algoritmo Diffie-Hellman;

Número de Identificação Pessoal (Personal Identification Number - PIN): um código alfanumérico ou senha usada para autenticar uma identidade;

Número de Registro: Número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4];

Oficial de segurança: uma entidade ou processo que age como tal, realizando funções criptográficas de iniciação ou gerenciamento;

Parâmetros críticos de segurança (PCS): Representam informações sensíveis e relacionadas a segurança, tais como, chaves criptográficas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja divulgação ou modificação podem comprometer a segurança de um módulo criptográfico;

PC/SC: especificação para integração de cartões inteligentes (smart card) em sistemas de computação;

PKCS#11: padrão utilizado como interface para invocar operações criptográficas em hardware e é utilizado para prover suporte aos tokens.

Registro: Cadeia (string) de bytes que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].

Safesign: software gerenciador responsável pela identificação e manutenção dos certificados disponíveis em um hardware criptográfico (cartão inteligente ou Token USB);

Senha: uma cadeia de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar autorizações de acesso.

Software: Programas e componentes de dados usualmente armazenados em mídias que podem ser apagadas (disco rígido, por exemplo), os quais podem ser dinamicamente escritos e modificados durante a execução.

Token: Nome geral de todos os dispositivos criptográficos, tais como cartões inteligentes (smart cards), dispositivos que possuem senhas e funcionalidades de armazenamento de certificados etc.

Token USB PKI: dispositivo criptográfico portável integrado com smart card e porta USB. Uma das vantagens deste dispositivo sobre os cartões inteligentes é a portabilidade, bem como suporte a aplicações PKI.

Token USB: Dispositivo criptográfico com conector USB, portável e de fácil uso.

TSP (Token Service Provider): Camada de hardware abstrata presente no framework ePassNG. Esta camada interfaces comuns de entrada e saída para todos os tipos de dispositivos. O design pode prover uma determinada expansão contra as diferenças de hardware.

Transporte de chaves (key transport): Protocolo que possibilita que uma chave simétrica seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

Unidade de Dado: O menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].

Usuário: um indivíduo ou processo que age como tal com o intuito de obter acesso a um módulo criptográfico para executar serviços.

2. Lista de Acrônimos

AES Advanced Encryption Standard

APDU Application Protocol Data Unit

API Application Programming Interface

ATR Answer To Reset

CBC Cipher Block Chaining

CE Consumer electronics

CFCA China Financial Certificate Authority

CLK Clock

DES Data Encryption Standard

DF Dedicated File

EEPROM Electrically Erasable Programmable Read-Only Memory

EF Elementary File

FCC Federal Communications Commission

FIPS Federal Information Processing Standards

GND Ground

ICC Integrated Circuit Chip

ICP Infra-Estrutura de Chaves Públicas

ICP-Brasil Infra-Estrutura de Chaves Públicas Brasileira

IEC International Electrotechnical Commission

IKE Internet key exchange

IN Instrução Normativa

IPSec Internet Protocol Security

I/O Input/Output

ISO Internation Organization for Standardization

ITL Information Technology Laboratory

ITI Instituto Nacional de Tecnologia da Informação

IV Initialization Vector

JCE Java Cryptography Extension

LCR Lista de Certificados Revogados

LEA Laboratório de Ensaios e Auditoria

LSITEC Laboratório de Sistemas Integráveis Tecnológico

MAC Message Authentication Code

MF Master File

MSCAPI Microsoft Crypto API

NIST National Institute of Standards and Technology

OPSEC Operations security

PC Personal Computer

PCS Parâmetros Críticos de Segurança

PIN Personal Identification Number

PPS Protocol and Parameters Selection

PUK PIN Unlock Key

RFU Reserved for Future Use

RNG Random Number Generator

RSA Rivest Shamir and Adleman

RST Reset

SHA Secure Hash Algorithm

SO Sistema Operacional

SP Service Provider

SSL Secure Sockets Layer

TLV Tag Length Value

TSP Token Service Provider

TTL Time To Live

USB Universal Serial Bus

VPP Variable Supply Voltage

3. Sobre a Pronova Soluções Inteligentes

A Pronova Soluções Inteligentes é formada por uma equipe com mais de 15 anos de experiência no mercado de Segurança da Informação. Somos pioneiros neste setor, no qual sempre nos destacamos pela qualidade dos produtos que oferecemos aliada ao bom atendimento, formação de parcerias, lançamento de novas tecnologias, além de serviços de consultoria.

Ao longo deste período, lançamos e comercializamos no Brasil produtos desenvolvidos e utilizados em larga escala no mercado internacional. Atendemos as mais variadas necessidades de proteção, como armazenamento e transmissão segura de informações, monitoramento de conteúdo hostil, além de proteção de software contra pirataria, entre outros.

4. Sobre o ProToken Plus

O ProToken Plus é o primeiro modelo de Token USB Pronova com 32Kb de memória, com suporte a RSA 2048bits e SHA-2 que utiliza o middleware SafeSign da AET.

4.1 Visão Geral do Produto

Cordão para transporte

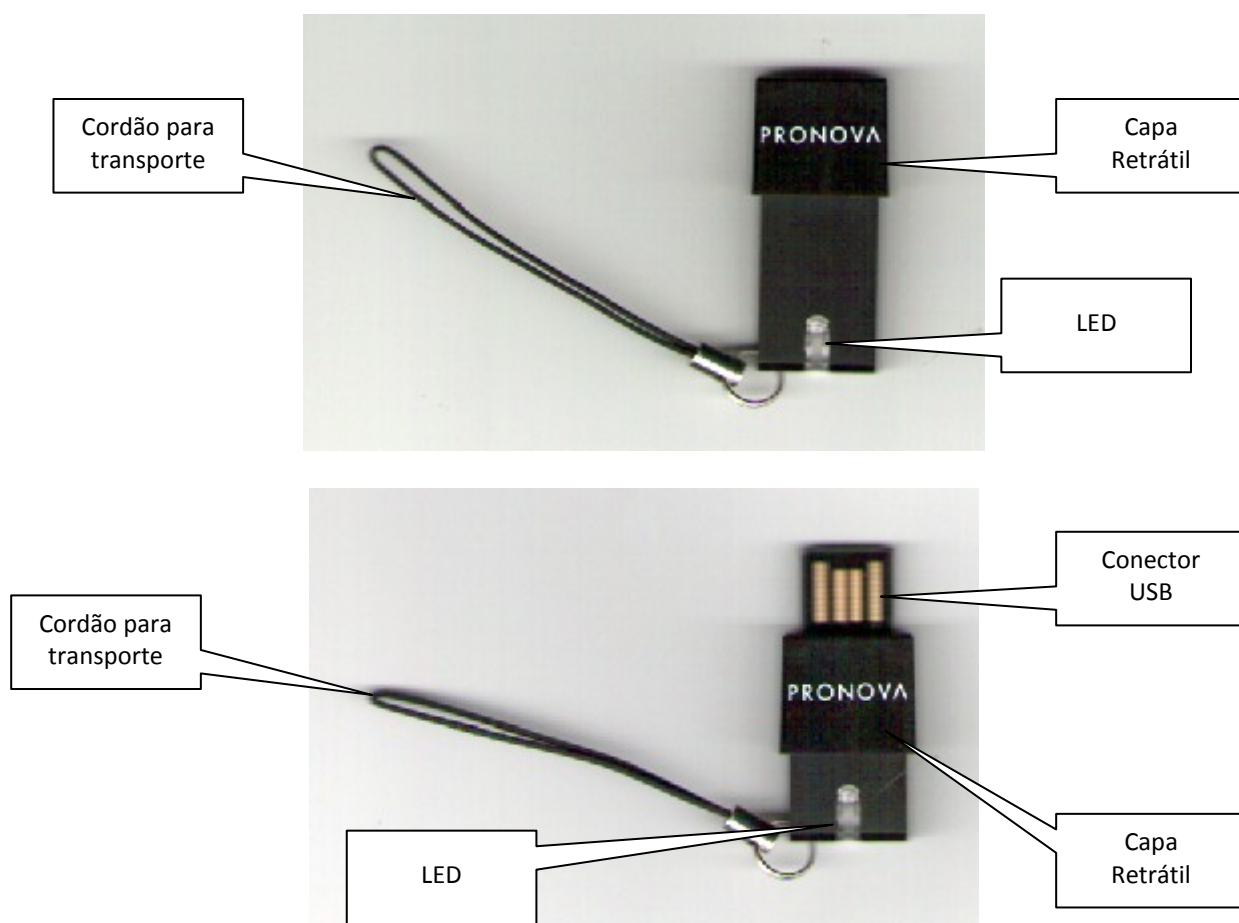
Capa Retrátil

LED

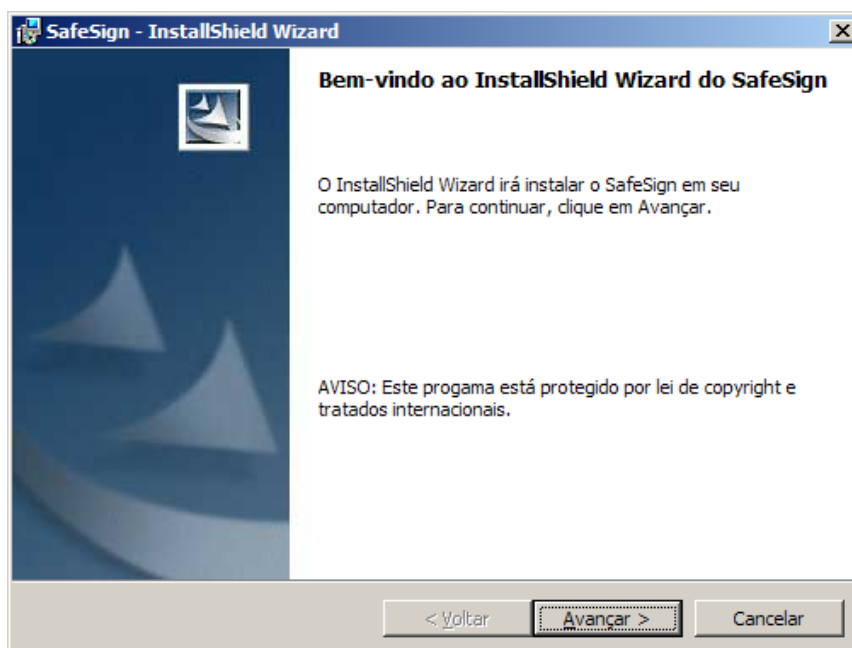
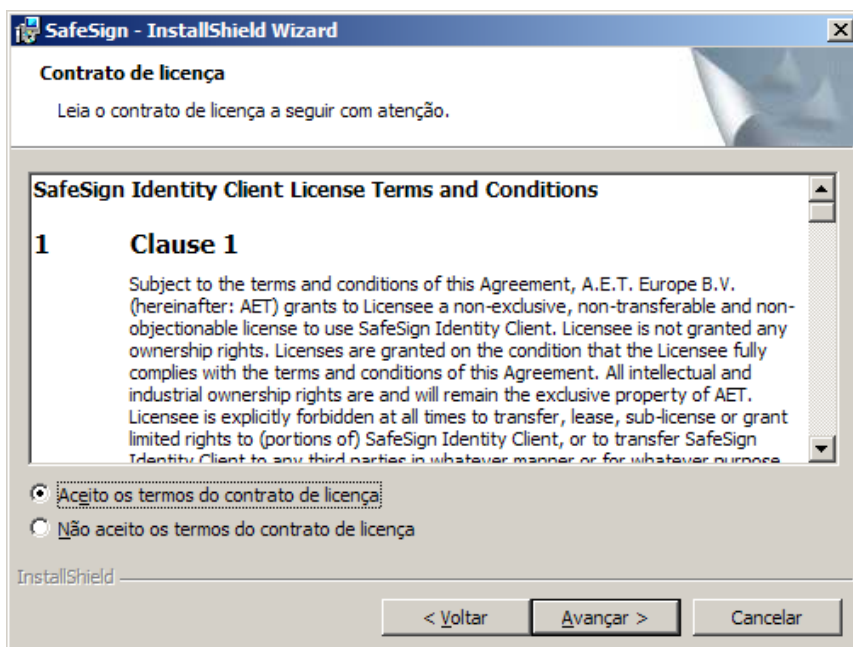
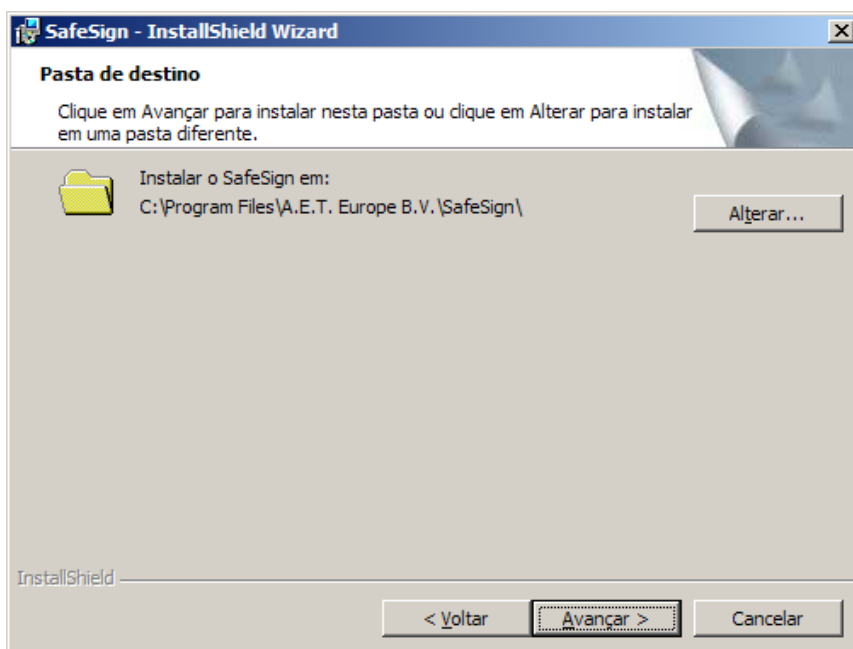
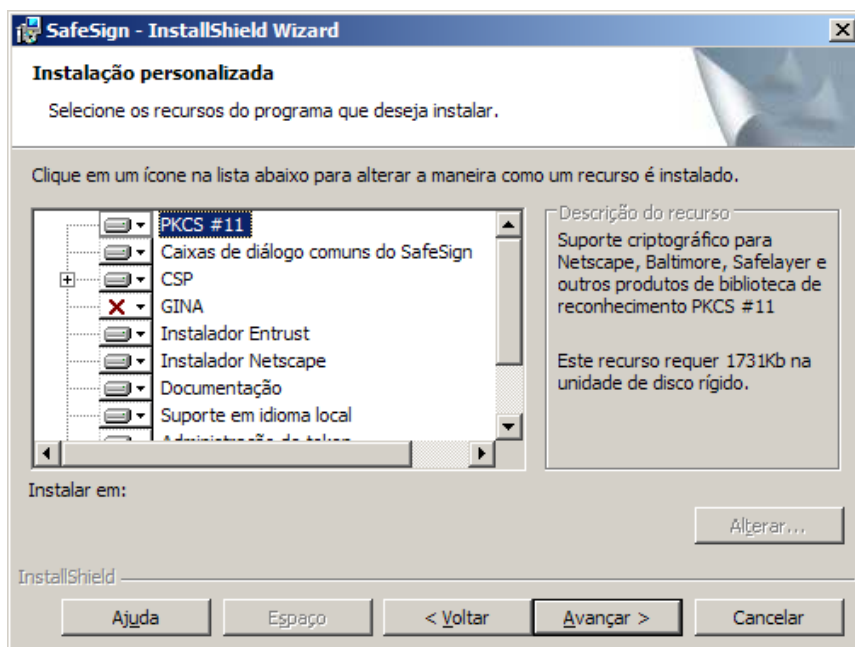
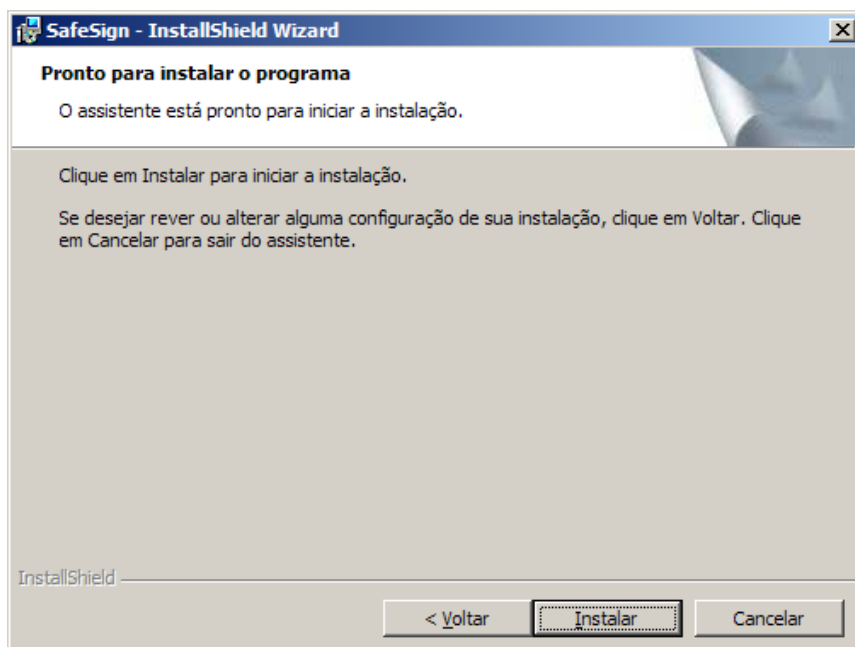
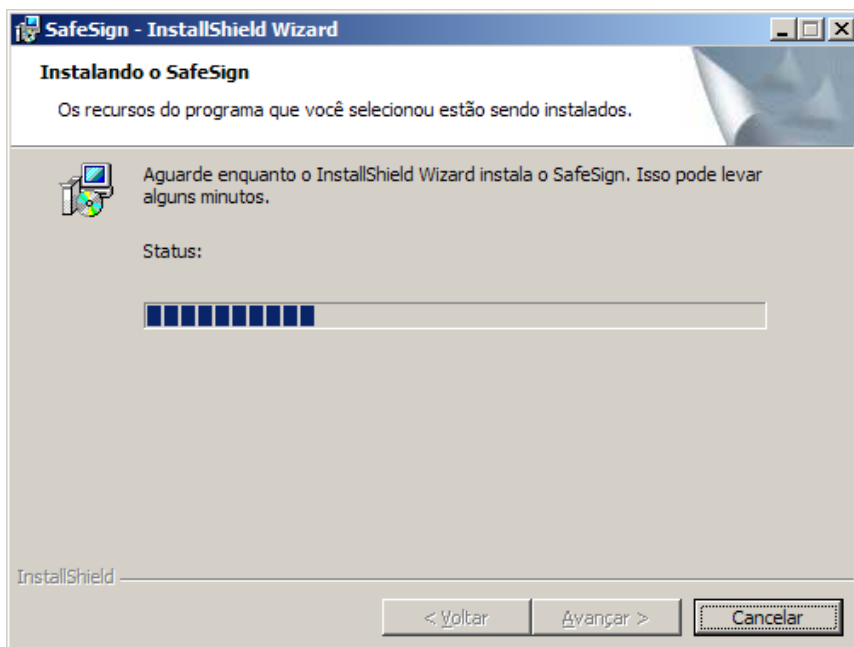
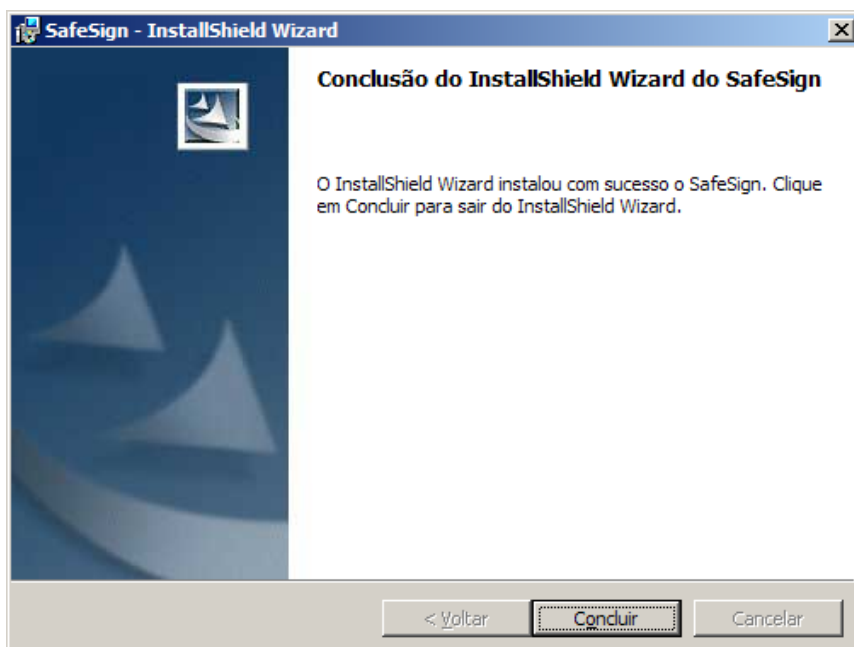
Conector USB

Cordão para transporte

LED

Capa Retrátil

5. Instalando o software SafeSign Identity Client

Ao executar o arquivo de instalação SafeSign-Identity-Client, você poderá selecionar o idioma a ser utilizado durante a instalação. Após selecionar o idioma desejado, clique no botão OK para continuar.

Depois de selecionar o idioma, será iniciado o assistente de instalação do SafeSign. Para continuar, clique no botão Avançar.

Na próxima janela, selecione a opção “Aceito os termos do contrato de licença” e clique no botão Avançar.

Na próxima janela, o assistente irá informar o local onde serão instalados os arquivos do SafeSign. Para continuar, clique no botão Avançar.

Na próxima janela, não faça nenhuma modificação, apenas clique o botão Avançar para continuar.

Agora que todas as configurações estão definidas, clique no botão Instalar.

Aguarde a cópia dos arquivos para o disco rígido do seu computador.

Assim que a transferência dos arquivos for concluída, a seguinte janela será exibida. Clique no botão Concluir para finalizar a instalação.

6. A primeira utilização do ProToken Plus

Não existe nenhuma necessidade de se inicializar o ProToken Plus, pois ele já vem formatado de fábrica. O valor padrão tanto para o PIN como para o PUK é "12345678" (sem as aspas) e existe um número máximo de acerto tanto para o PIN como para o PUK. Este número é de 5 (cinco) tentativas.

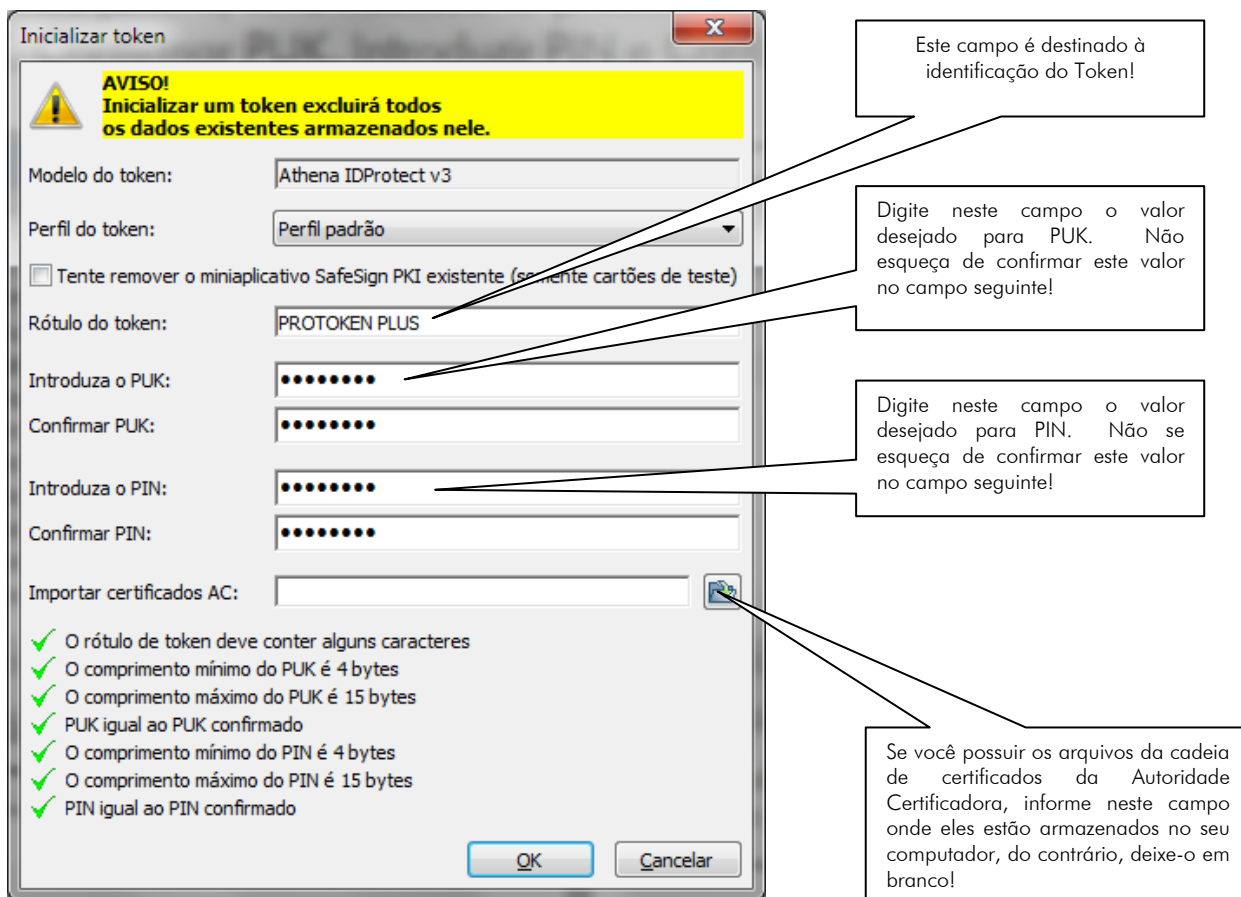
Contudo, você poderá inicializar o seu ProToken Plus sempre que desejar. Todavia, antes de inicializar o seu ProToken Plus, é necessário saber que:

a) Para inicializar é necessário estar de posse do valor do PUK, do contrário não será possível inicializar o seu ProToken Plus;

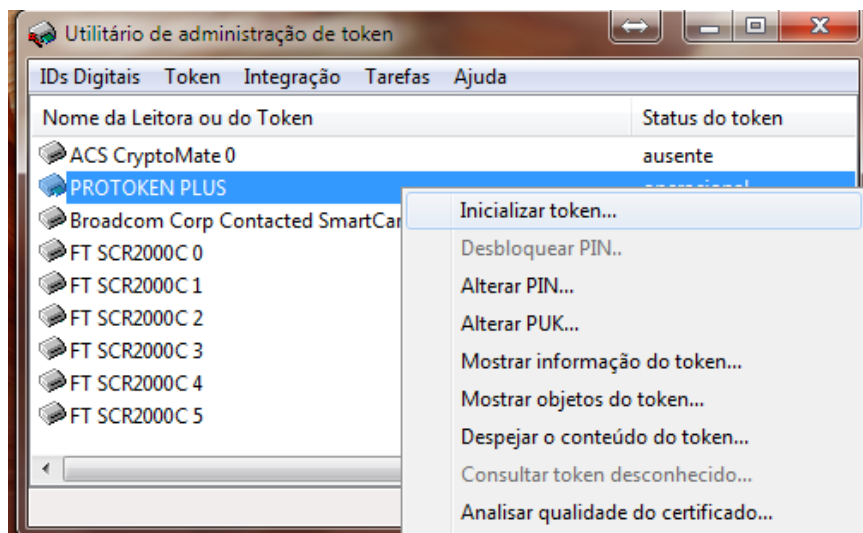
b) A função inicializar VAI APAGAR TODAS AS INFORMAÇÕES GRAVADAS, INCLUSIVE CERTIFICADOS DIGITAIS E SEUS RESPECTIVOS PARES DE CHAVES, DA MEMÓRIA DO PROTOKEN PLUS E NÃO SERÁ POSSÍVEL RECUPERAR ESTAS INFORMAÇÕES!

c) Se ocorrer cinco tentativas mal sucedidas de acerto do PUK, o PROTOKEN PLUS SERÁ TOTALMENTE BLOQUEADO E NÃO PODERÁ SER REUTILIZADO E COM ISSO TODOS OS DADOS GRAVADOS NELE ESTARÃO PERDIDOS.

d) A garantia do produto não cobre troca do dispositivo em função do bloqueio do PUK. Desta forma, CUIDADO PARA NÃO EXCEDER AS TENTATIVAS DE ACERTO DO PUK.

Se você estiver seguro de que deseja realmente inicializar o seu ProToken Plus, siga as próximas instruções. Se não estiver seguro desta decisão, não inicialize o seu dispositivo!

1. Carregar a ferramenta Administração do Token (INICIAR → PROGRAMAS → SAFESIGN STANDARD)

2. Insira o Token USB em uma porta USB livre e aguarde que ele seja reconhecido pelo Windows. Assim que o Token USB for reconhecido, observe que será exibido na coluna Leitor ou nome de token o texto: PROTOKEN PLUS. Na coluna Status do token: operacional.

3. Clique com o botão direito do mouse sobre a linha onde está escrito Token em braço e selecione a opção Inicializar token...

4. Antes de clicar no botão OK desta janela, será necessário preencher os campos Rótulo de token, Introduza o PUK, Confirmar PUK, Introduzir PIN e Confirmar PIN.

Inicializar token

AVISO!
Inicializar um token excluirá todos os dados existentes armazenados nele.

Modelo do token: Athena IDProtect v3

Perfil do token: Perfil padrão

Tente remover o miniaplicativo SafeSign PKI existente (somente cartões de teste)

Rótulo do token: PROTOKEN PLUS

Introduza o PUK: ••••••••

Confirmar PUK: ••••••••

Introduza o PIN: ••••••••

Confirmar PIN: ••••••••

Importar certificados AC:

- O rótulo de token deve conter alguns caracteres
- O comprimento mínimo do PUK é 4 bytes
- O comprimento máximo do PUK é 15 bytes
- PUK igual ao PUK confirmado
- O comprimento mínimo do PIN é 4 bytes
- O comprimento máximo do PIN é 15 bytes
- PIN igual ao PIN confirmado

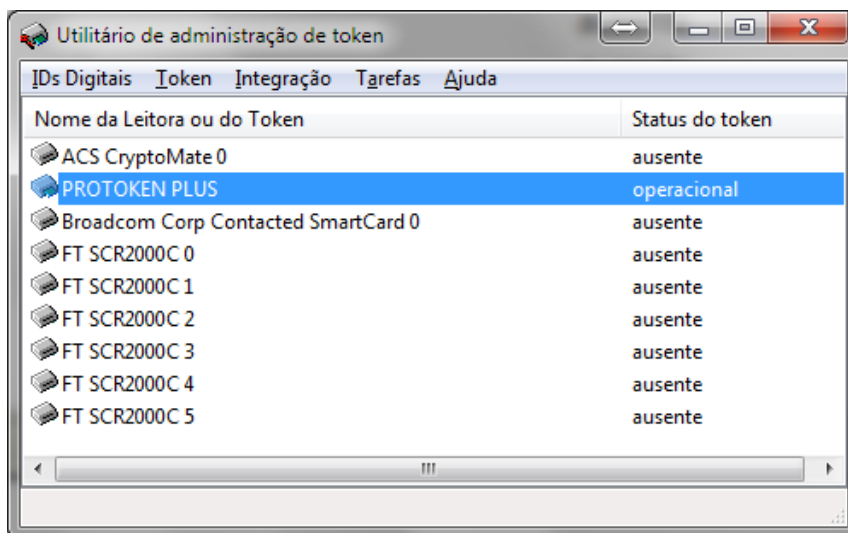
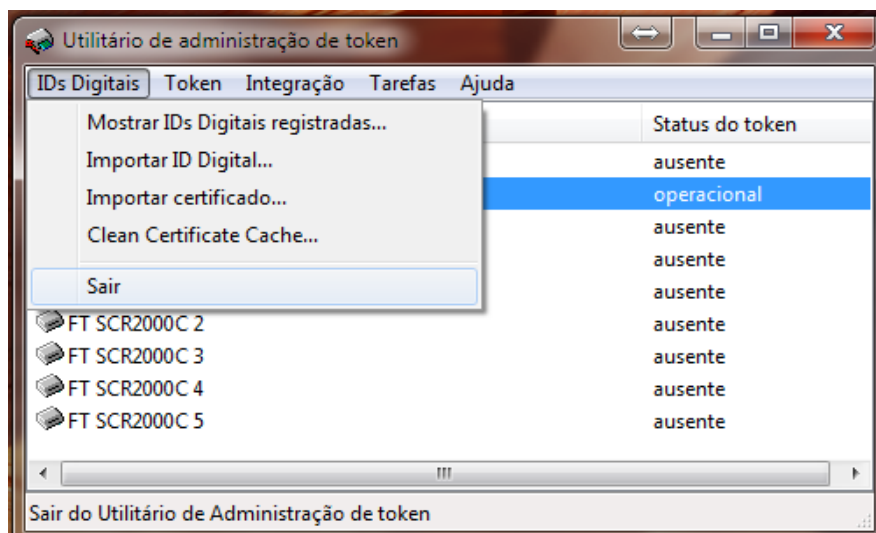
OK Cancelar

Este campo é destinado à identificação do Token!

Digite neste campo o valor desejado para PUK. Não esqueça de confirmar este valor no campo seguinte!

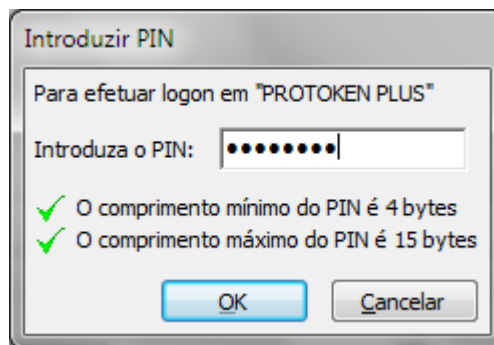
Digite neste campo o valor desejado para PIN. Não se esqueça de confirmar este valor no campo seguinte!

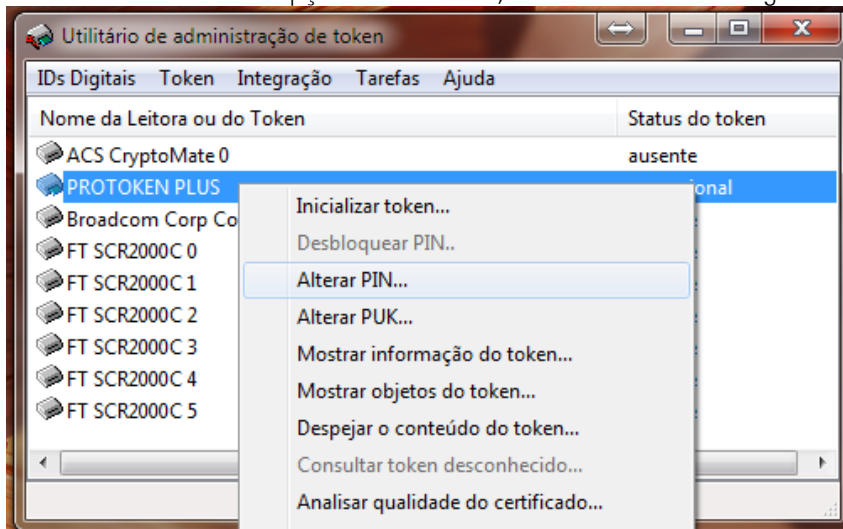
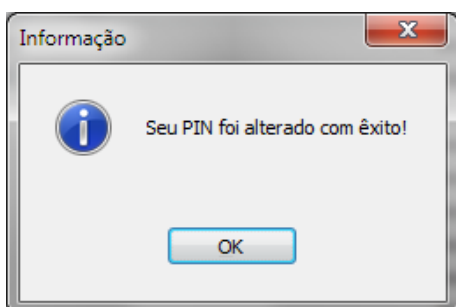
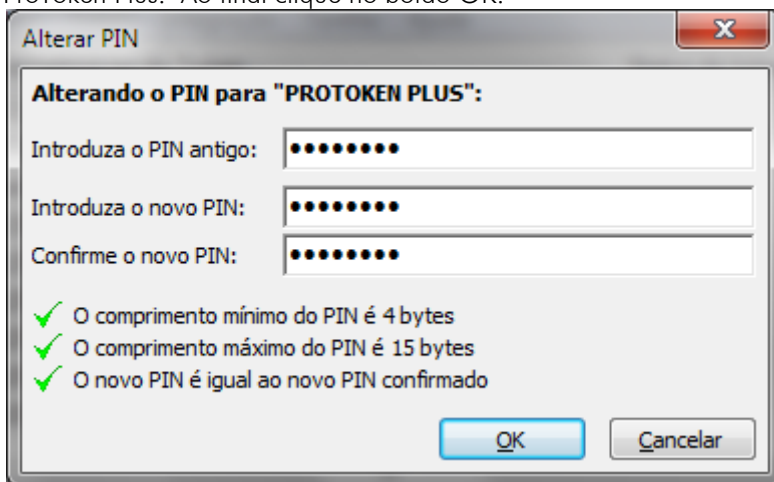
Se você possuir os arquivos da cadeia de certificados da Autoridade Certificadora, informe neste campo onde eles estão armazenados no seu computador, do contrário, deixe-o em branco!

5. Ao final observe que o dado informado no campo Rótulo de token será exibido na coluna Leitor ou nome de token. Uma vez que o cartão inteligente foi inicializado o status será operacional.

Para fechar o Utilitário de administração de token, clique no botão fechar (X no canto superior direito da janela) ou se preferir, clique em Códigos digitais da barra de menu e por fim, selecione a opção Sair.

Agora seu ProToken Plus acaba de ser re-inicializado (re-formatado) e está pronto para fazer a solicitação de seu certificado digital ICP-Brasil. Com ele conectado ao computador acesse o site da Autoridade Certificadora e faça a solicitação do certificado digital.

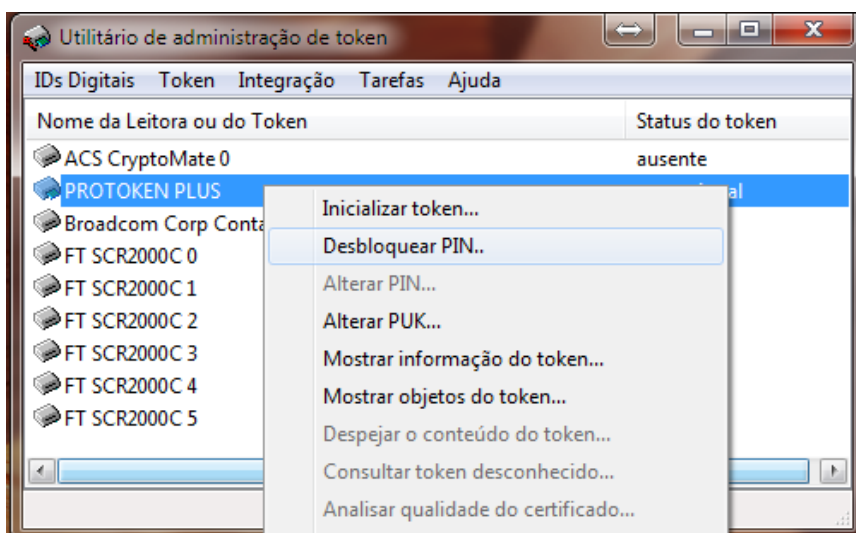
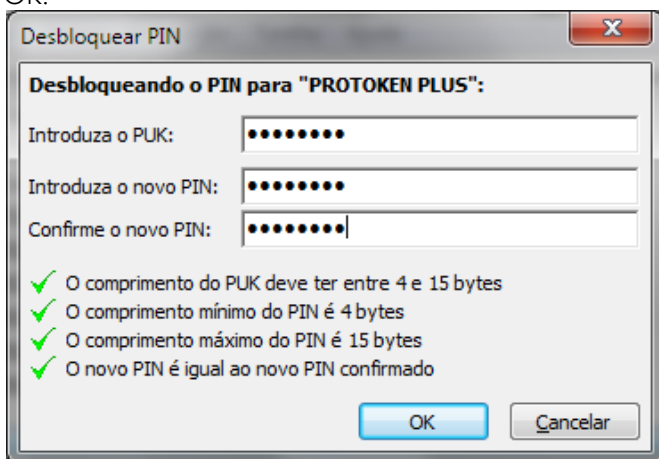
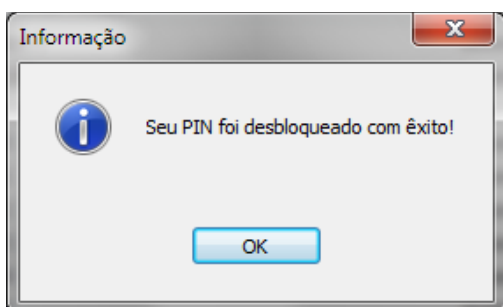
ATENÇÃO: ao ser questionado qual CSP (Provedor de Serviços de Criptografia) a ser utilizado, selecione a opção SafeSign Standard Cryptographic Service Provider.

Em determinado momento, será necessário informar o PIN do seu ProToken Plus, como demonstrado na imagem a seguir.

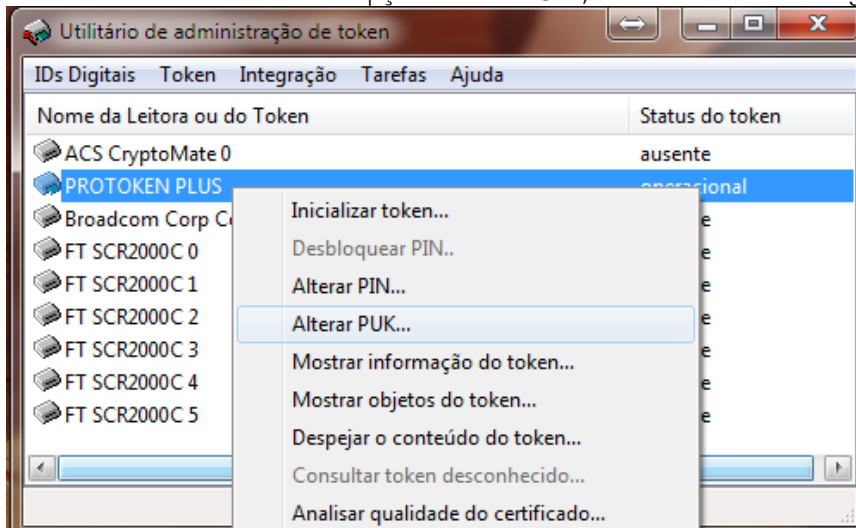
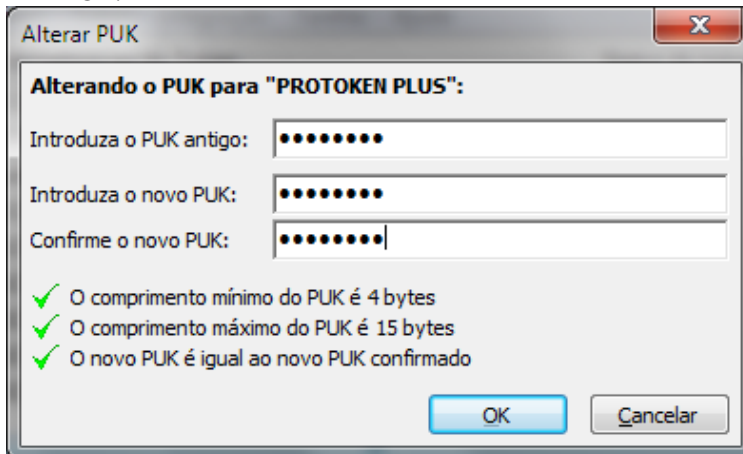
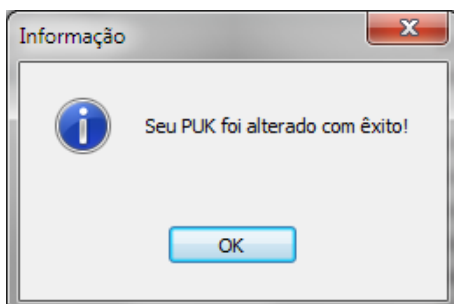
No campo Introduzir PIN, digite o PIN do seu cartão. Para continuar, clique no botão Verificar.

7. Alterando o PIN do ProToken Plus

Para alterar o PIN do ProToken Plus, carregue o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção "Alterar PIN", como ilustrado na imagem abaixo.

Em seguida, na janela Alterar PIN, digite o atual PIN e nos campos seguintes o Novo PIN para o seu ProToken Plus. Ao final clique no botão OK.

Esta é a mensagem que será exibida ao final desta operação.

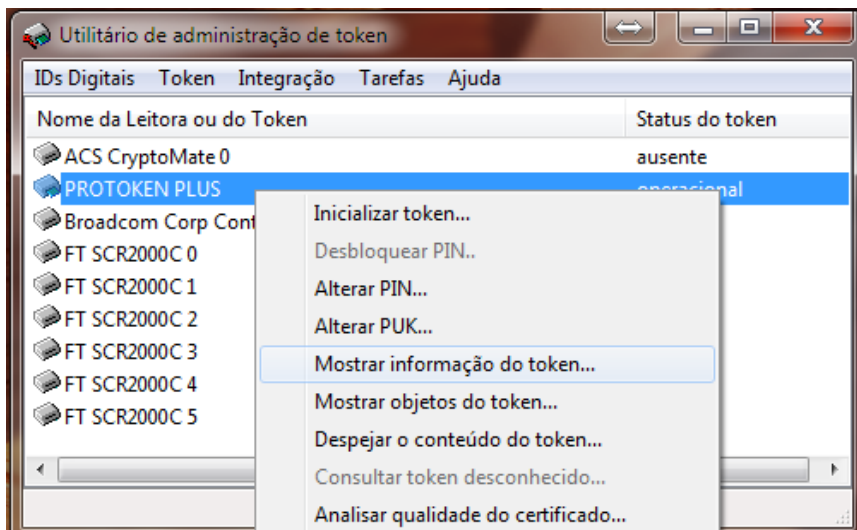
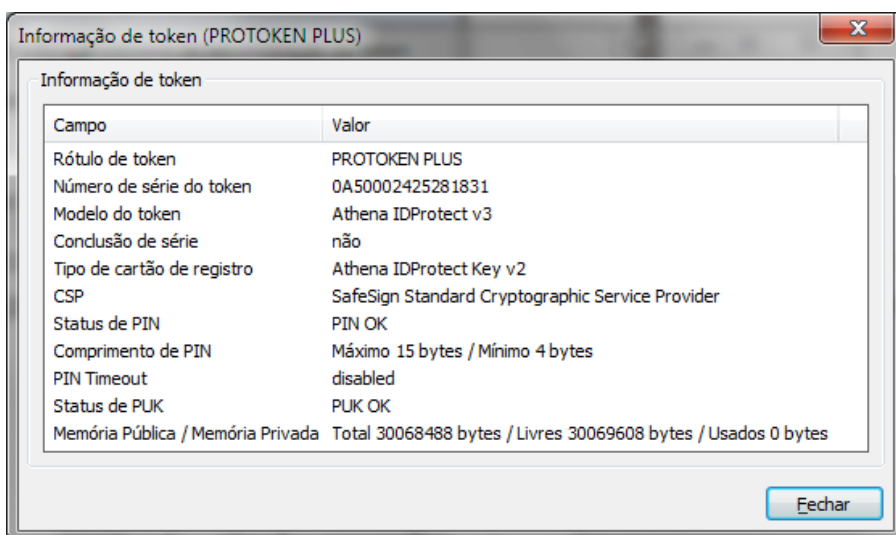
8. Destravando o PIN do ProToken Plus

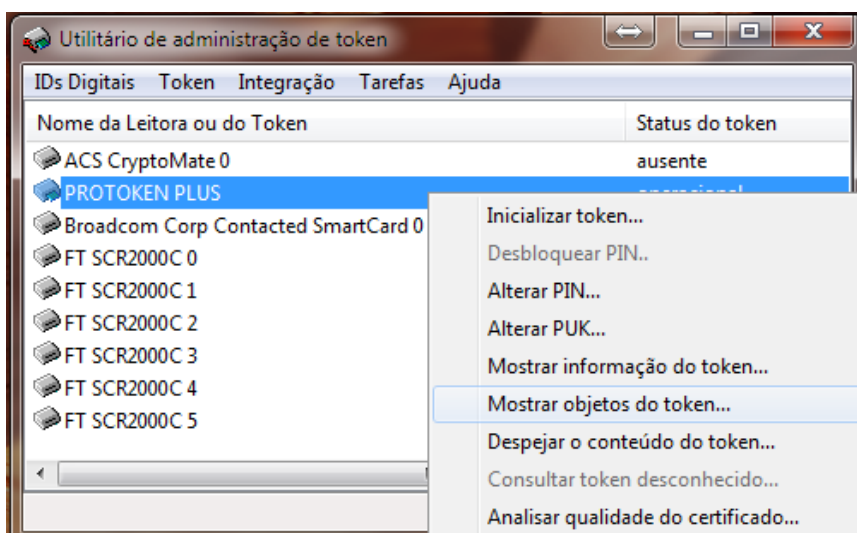
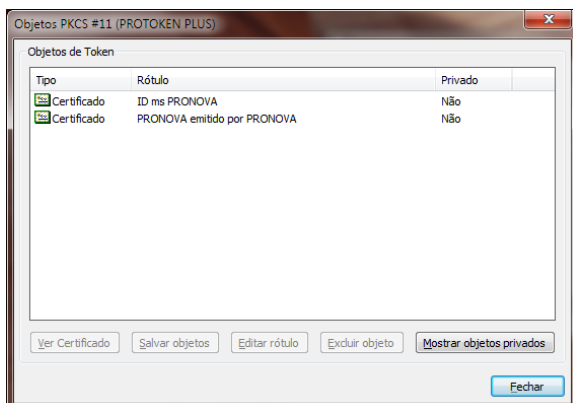
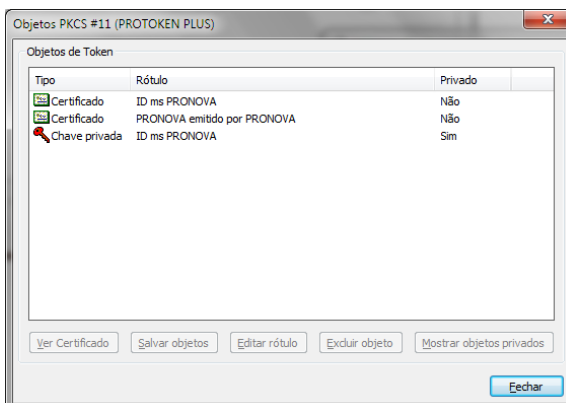
Caso você tenha excedido as tentativas de acerto do PIN e tenha recebido a mensagem de que o PIN está bloqueado, não se preocupe, através da função Desbloquear PIN você poderá redefinir um PIN para o seu ProToken Plus. Para debloquear o PIN abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção "Desbloquear PIN", como ilustrado na imagem abaixo.

Na janela Desbloquear PIN, digite no primeiro campo o atual PUK do seu ProToken Plus e nos campos seguintes o PIN desejado para o seu dispositivo. Uma vez preenchidos estes campos, clique no botão OK.

Cuidado, não digite o PUK incorreto!

Esta é a mensagem que será exibida ao final desta operação.

9. Alterando o PUK do ProToken Plus

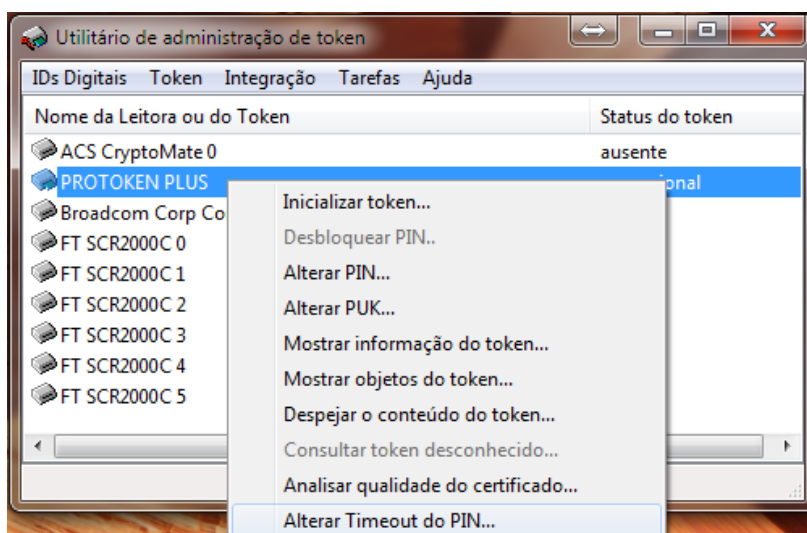
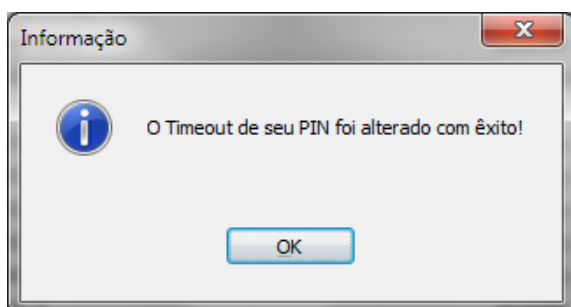
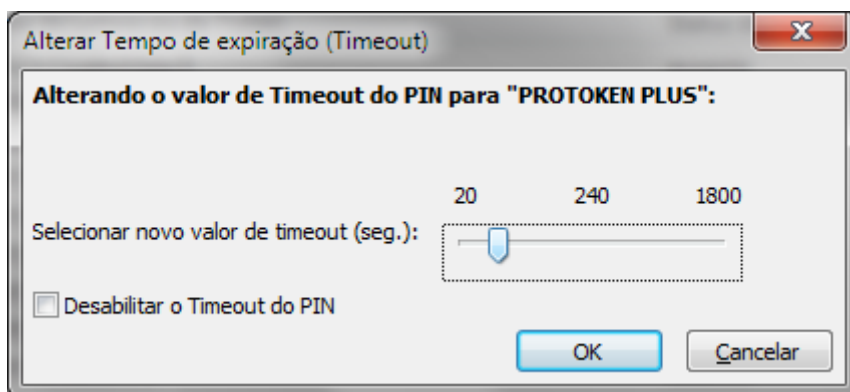
Para ampliar a segurança do seu certificado digital, recomendamos que o PUK de fábrica seja alterado. Se você desejar alterar o PUK do seu dispositivo, abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção "Alterar PUK", como ilustrado na imagem abaixo.

Na janela Alterar PUK, digite no primeiro campo o atual PUK do seu ProToken Plus e nos campos seguintes o novo PUK desejado para o seu dispositivo. Uma vez preenchidos estes campos, clique no botão OK.

Cuidado, não digite o PUK incorreto!

Esta é a mensagem que será exibida ao final desta operação

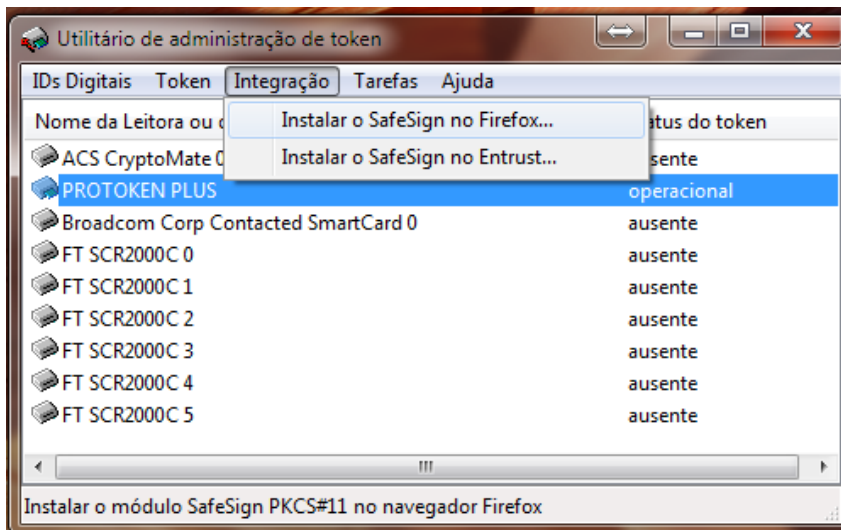
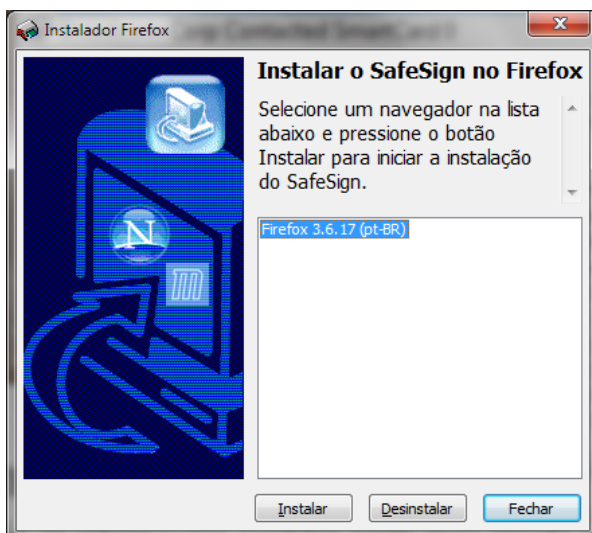
10. Visualizando as Informações do ProToken Plus

Para visualizar as informações do ProToken Plus, abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção “Alterar PUK”, como ilustrado na imagem abaixo.

Uma janela chamada Informação de token será exibida. Nesta janela será possível visualizar informações sobre o seu dispositivo, dentre elas o número de série, o CSP e a quantidade de memória do dispositivo. Para fechar esta janela, basta clicar no botão “Fechar”.

11. Visualizando os objetos gravados na memória do ProToken Plus

Para saber se dentro do seu ProToken Plus existe ou não certificados digitais, abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção "Mostrar objetos do token", como ilustrado na imagem abaixo.

Uma janela chamada Objetos PKCS#11 será exbida, nela você poderá visualizar se certificados e chaves estão gravados na memória do seu dispositivo. Para visualizar a presença de uma chave privada, clique no botão "Mostrar objetos privados", todavia, será necessário informar o PIN do seu ProToken Plus.

Objetos Públicos | Objetos Públicos e Privados

12. Controlando o tempo de vida do PIN

Se existir a necessidade de habilitar o controle do tempo de vida do PIN que por padrão fica desabilitado, abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção "Alterar Timeout do PIN", como ilustrado na imagem abaixo.

Na janela Alterar Tempo de expiração (Timeout) desabilite a opção "Desabilitar o Timeout do PIN e ajuste o tempo em segundos desejado. Por fim, clique no botão OK para confirmar este ajuste. Desta forma, se você configurou 240 segundos, a cada 4 minutos, será necessário digitar novamente o PIN do ProToken Plus.

13. Integração com Mozilla Firefox

Para que seja possível a utilização do ProToken Plus no navegador Mozilla Firefox, é necessário proceder a integração do módulo PKCS#11 SafeSign neste navegador. Para tanto, abra o Utilitário de Administração, clique com o botão direito do mouse e selecione a opção “Alterar Timeout do PIN”, como ilustrado na imagem abaixo.

Na janela Instalador Firefox, selecione a versão do navegador instalado no seu computador e em seguida, clique no botão “Instalar”. Ao final, clique no botão “Fechar”.

14. Suporte Técnico

Se as informações contidas neste guia rápido não foram suficientes, não se preocupe, entre em contato conosco sempre que precisar. O telefone para contato é (21) 2491-3688 e o nosso chat está em www.pronova.com.br.